(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 130 843 A3

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
23.07.2003 Bulletin 2003/30

(43) Date of publication A2:
05.09.2001 Bulletin 2001/36

(21) Application number: **00128248.2**

(22) Date of filing: **21.12.2000**

(51) Int Cl.[7]: **H04L 9/30**, H04L 9/08

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.12.1999 US 469487**

(71) Applicant: **ContentGuard Holdings, Inc.**
Wilmington, Delaware 19803 (US)

(72) Inventors:
- **Wang, Xin**
  Los Angeles, CA 90007 (US)
- **Ta, Thanh T.**
  Huntington Beach, CA 92648 (US)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) **System and method for transferring the right to decode messages in a symmetric encoding scheme**

(57) Methods for transferring among key holders in encoding and cryptographic systems the right to decode and decrypt messages in a way that does not explicitly reveal decoding and decrypting keys used and the original messages. Such methods are more secure and more efficient than typical re-encoding and re-encryption schemes, and are useful in developing such applications as document distribution and long-term file protection.

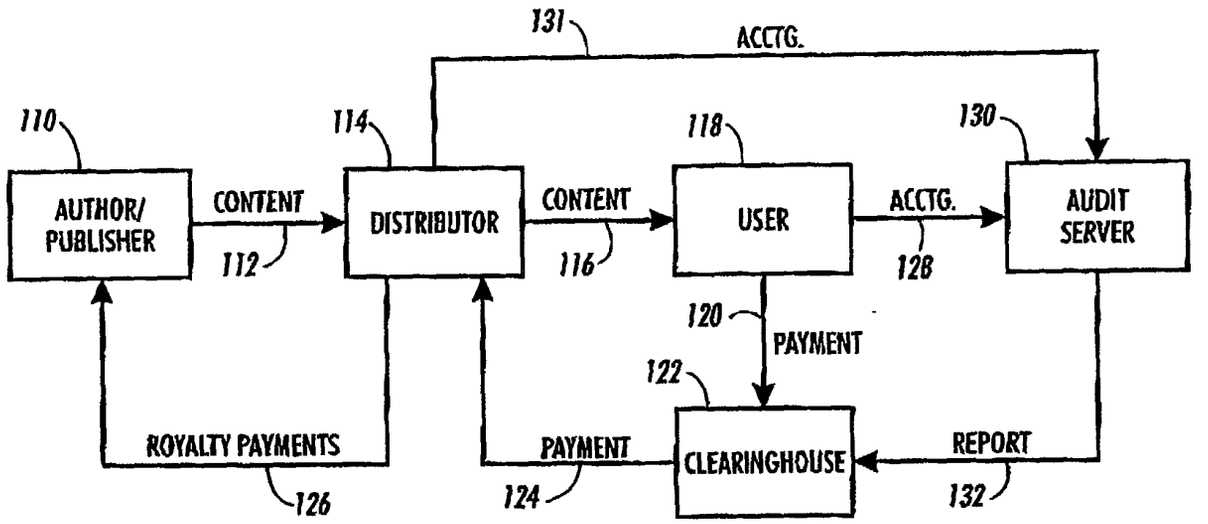

FIG. 1

EP 1 130 843 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 12 8248

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	MAMBO M ET AL: "Protection of data and delegated keys in digital distribution" , INFORMATION SECURITY AND PRIVACY. SECOND AUSTRALIAN CONFERENCE, ACISP'97. PROCEEDINGS, INFORMATION SECURITY AND PRIVACY. SECOND AUSTRALIAN CONFERENCE, ACISP '97. PROCEEDINGS, SYDNEY, NSW, AUSTRALIA, 7-9 JULY 1997 , 1997, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 271 - 282 XP008016393 ISBN: 3-540-63232-8 * page 272, line 9 - line 20 * * page 275, line 8 - page 276, line 22 * ---	1-7,11	H04L9/30 H04L9/08
A	WO 99 34553 A (V ONE CORP) 8 July 1999 (1999-07-08) * page 1, line 5 - line 12 * * page 13, line 14 - line 21 * * page 20, line 23 - page 21, line 6 * * page 21, line 16 - page 22, line 10 * * page 22, line 18 - line 23 * ---	1-11	
D,A	BLAZE, M., STRAUSS, M.: "Atomic Proxy Cryptography" DRAFT, [Online] 2 November 1997 (1997-11-02), XP002239619 Retrieved from the Internet: <URL:ftp://ftp.research.att.com/dist/mab/proxy.ps> [retrieved on 2003-04-28] * page 5, line 9 - last line * -----	1-11	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	28 April 2003	Liebhardt, I

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 12 8248

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-04-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9934553 A	08-07-1999	US 6084969 A	04-07-2000
		AU 1946699 A	19-07-1999
		WO 9934553 A1	08-07-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82